WHAT IS CLAIMED IS:

1. A method for secure message reception from a plurality of remote devices, comprising:

receiving a message;

obtaining a reverse channel address associated with the received message

ensuring that the received message is associated with at least one of the remote devices;

determining the destination address for the received message by obtaining a reverse channel address associated with the received message; and

routing the message to the destination address.

2. The method of claim 1, wherein the communications protocol employed to transmit the received message is the ReFLEX protocol.

3. The method of claim 1, wherein the step of ensuring further comprises:

reviewing header information in the received message.

4. The method of claim 3, wherein the determining step further comprises:

retrieving a remote device profile based upon the obtained reverse channel address.

5. The method of claim 4, wherein the determining step further comprises:

obtaining the destination address from a remote device.

6. The method of claim 1, wherein the determining step further comprises:

determining whether the encrypted message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server.

7. The method of claim 6, wherein the encrypted message is routed to a hosted crypto server.

8. The method of claim 6, wherein the encrypted message is routed to an enterprise crypto server.

9. A method for establishing encryption keys with a data center from a remote wireless device, comprising the steps of:

when an event occurs, automatically sending a first registration message to the data center;

receiving, in response to the first registration message, an acknowledgment; and

when the acknowledgment is received, sending a second registration message to said data center, wherein the second registration message includes a command to start encryption key establishment.

10. The method of claim 9, wherein the key establishment is achieved with a ReFLEX protocol.

11. The method of claim 9, wherein the event is an initial powering on of the remote wireless device.

12. The method of claim 9, wherein the event is an indication that a predetermined error has occurred with the remote wireless device.

13. The method of claim 9, wherein during encryption key establishment, the second registration message can be sent to said data center, and wherein the second registration message includes a wait command.

14. The method of claim 13, wherein the wait command requests the data center to wait for a signature key.

15. The method of claim 13, wherein the wait command requests the data center to wait for an ephemeral key.

16. The method of claim 9, wherein during encryption key establishment, the second registration message can be sent to said data center, and wherein the second registration message includes a send command.

17. The method of claim 16, wherein the wait command requests the data center to wait for a signature key.

18. The method of claim 16, wherein the wait command requests the data center to wait for an ephemeral key.

19. The method of claim 9, further comprising:

sending an ephemeral key command from said data center to said remote device, wherein said command includes at least one of a server initialization vector and a remote device initialization vector.

20. An apparatus for secure message reception from a plurality of remote devices, comprising:

means for receiving a message;

means for obtaining a reverse channel address associated with the received message

means for ensuring that the received message is associated with at least one of the remote devices;

means for determining the destination address for the received message by obtaining a reverse channel address associated with the received message; and

means for routing the message to the destination address.

21. The apparatus of claim 20, wherein the communications protocol employed to transmit the received message is the ReFLEX protocol.

22. The apparatus of claim 20, wherein the means for ensuring further comprises:

means for reviewing header information in the received message.

23. The apparatus of claim 22, wherein the means for determining further comprises:

means for retrieving a remote device profile based upon the obtained reverse channel address.

24. The apparatus of claim 23, wherein the means for determining further comprises:

means for obtaining the destination address based upon the remote device profile.

25. The apparatus of claim 20, wherein means for determining further comprises:

means for determining whether the encrypted message is associated with a remote device that is associated with a hosted crypto server or an enterprise crypto server.

26. The apparatus of claim 25, wherein the encrypted message is routed to a hosted crypto server.

27. The apparatus of claim 25, wherein the encrypted message is routed to an enterprise crypto server.

28. An apparatus for establishing encryption keys with a data center from a remote wireless device, comprising the steps of:

means for automatically sending a first registration message to the data center when an event occurs;

means for receiving, in response to the first registration message, an acknowledgment; and

means for sending a second registration message to said data center, wherein the second registration message includes a command to start encryption key establishment.

29. The apparatus of claim 28, wherein the event is an initial powering on of the remote wireless device.

30. The apparatus of claim 28, wherein the event is an indication that a predetermined error has occurred with the remote wireless device.

31. The apparatus of claim 28, wherein during encryption key establishment, the second registration message can be sent to said data center, and wherein the second registration message includes a wait command.

32. The apparatus of claim 28, wherein during encryption key establishment, the second registration message can be sent to said data center, and wherein the second registration message includes a send command.

33. The apparatus of claim 28, further comprising:

sending an ephemeral key command from said data center to said remote device, wherein said command includes at least one of a server initialization vector and a remote device initialization vector.